

# RESTRICTIONS ON INTERNET FREEDOMS

RECOMMENDATIONS FOR THAI POLICY-MAKERS AND CIVIL SOCIETY



---

# **RESTRICTIONS ON INTERNET FREEDOMS**

Recommendations for Thai Policy-makers and Civil Society

2023

Asia Centre

---

---

Copyright © 2023 Asia Centre. All rights reserved.

Permission Statement: No part of this report in printed or electronic form may be reproduced, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying or otherwise, without written permission of the Asia Centre.

Copyright belongs to Asia Centre unless otherwise stated.

Civil society organisations and educational institutions may use this report without requesting permission on the strict condition that such use is not for commercial purposes.

When using or quoting this report, every reasonable attempt must be made to identify the copyright owners.

Errors or omissions will be corrected in subsequent editions.

Requests for permission should include the following information:

- The title of the document for which permission to copy material is desired.
- A description of the material for which permission to copy is desired.
- The purpose for which the copied material will be used and the manner in which it will be used.
- Your name, title, company or organisation name, telephone number, e-mail address and mailing address.

Please send all requests for permission to:

**Asia Centre**

65/168, Chamnan Phenjati Business Center Building 20th  
Floor, Rama 9 Road, Huai Kwang, Huai Kwang,  
Bangkok, 10310, Thailand  
[contact@asiacentre.org](mailto:contact@asiacentre.org)

---

# CONTENTS

	Page
<i>Abbreviations</i> .....	IV
<i>Executive Summary</i> .....	V
<b>1. Introduction</b> .....	1
1a. Methodology .....	1
1b. The Internet and Thailand's Political Development .....	1
1c. Trust in Public Institutions .....	3
<b>2. Internet Freedoms Regulatory Measures</b> .....	4
2a. Legal Measures .....	4
Penal Code .....	4
Computer Crime Act .....	5
Internal Security Act .....	6
2b. Non-legal Measures .....	6
Information Operations .....	7
Targetted Surveillance .....	7
2c. Impacts .....	8
Persecution of Users .....	8
Denying Access to Information .....	9
Mental Health .....	9
Declining Trust in Public Institutions .....	10
<b>3. Policy Recommendations</b> .....	11
<b>4. Conclusion</b> .....	13
<i>Bibliography</i> .....	14

---

# ABBREVIATIONS

CCA	Computer Crime Act
CCPR	Human Rights Committee
CSO	Civil Society Organisation
ECT; EC	Election Commission of Thailand
EIP	Election Integrity Project
FFP	Future Forward Party
HRD	Human Rights Defender
ICCPR	International Covenant on Civil and Political Rights
(I)NGO	(International) Non-governmental Organisation
ISA	Internal Security Act
ISOC	Internal Security Operations Command
IOs	Information Operations
KPI	King Prajadhipok's Institute
MDES	Ministry of Digital Economy and Society
MFP	Move Forward Party
MIL	Media Information Literacy
MP	Member of Parliament
NCPO	National Council for Peace and Order
OHCHR	Office of the United Nations High Commissioner for Human Rights
PM	Progressive Movement
PPP	People's Power Party
PTP	Pheu Thai Party
TRT	Thai Rak Thai
UPR	Universal Periodic Review
UN	United Nations
US	United States

---



---

# EXECUTIVE SUMMARY

Since the mid-2010s, internet freedoms in Thailand have declined sharply and rapidly given that successive governments have tightened their control over the internet at the expense of a people- and rights-centred approach to the digital sphere. This has not only put internet freedoms in Thailand at stake; it has also challenged the prospects for a stronger and cohesive democratic system shaped equitably by all actors.

Internet usage in Thailand started to grow significantly in the mid-2000s, witnessing a remarkable increase in the number of internet users. In 2011, only 23.6% of the population had access to the internet, but by 2023, this number had skyrocketed to 88%. This substantial growth also corresponded with a considerable uptick in the use of social media, particularly via smartphones. As of early 2023, there were 52.25 million social media users, constituting 72.8% of the total population of 71.75 million. Notably, Facebook, TikTok, and Instagram stood out as the most popular social networking platforms.

The rapid development of the digital sphere has created a wide range of new opportunities for many non-state actors to engage actively in politics, primarily thanks to new and interactive means of instant communication and more capacity to mobilise people, online and offline. However, the popularity of the internet and social media also triggered governments to use legal and non-legal measures to gain and retain control over the digital sphere. This report analyses these governmental strategies by outlining the strategies themselves and by underscoring their impacts.

First, it outlines two types of strategies governments have used to control online activity, which have impacted internet freedoms. On the one hand, the use of legal provisions. Some of these provisions, like the Penal Code, are from the pre-digital era, while others, like the Computer Crime Act and the International Security Act, were passed in the context of the growing presence of the internet among people. Overall, the report shows how the legal ecosystem has systematically been used to curtail several civil liberties and political rights of many of those who try to keep government officials and policies accountable.

On the other hand, the use of non-legal measures, which have further contributed to allowing the government to remain in control of the country's digital activity. In such regard, information operations have emerged as a tactic to monitor and influence online discussions, aiming to discredit opponents, spread hate speech, and reinforce the establishment's power. The report also focuses on targeted surveillance, which has been used to access and gather personal data from a user's device without their interaction. The reasons behind its use include monitoring online activities, and protests, and seeking information about protest funding sources.

Individuals attempting to hold the government accountable often encounter prosecution and legal action, leading to a climate of fear and self-censorship that substantially hinders freedom of expression and media reporting. Simultaneously, authorities employ national security concerns to pressure tech companies into removing online content critical of the government. As a result, thousands of URLs have been removed, with major social media platforms like Facebook and Twitter complying with numerous requests to restrict content. These actions have contributed to a broader erosion of public trust in institutions, particularly the judiciary.

To address this issue and combat the overall decline in internet freedoms in the country, the report concludes with a set of policy recommendations aimed at various state and non-state actors. First, the international community is crucial in using international mechanisms, particularly UN mechanisms, to call out all forms of rights infringements in the online sphere. In parallel, the Thai government should intensify its efforts to implement the recommendations made by the international community and establish a digital environment that adheres to international human rights standards, while the Thai parliament should amend and repeal all laws that restrict internet freedoms. The ECT should collaborate with various stakeholders, especially tech companies, to ensure that digital media contributes to transparent elections. The NHRCT also plays a vital role in holding all relevant stakeholders accountable in cases of human rights violations in the digital sphere. CSOs are essential for monitoring and documenting rights violations in the online sphere and should continue to do so. Finally, tech companies should design user-friendly digital platforms that prioritise essential elements like privacy to ensure the respect of digital rights.

Only with a collective effort, the gaps that exist between different actors and people's limited trust towards some political actors can start to be addressed.

---

# 1. Introduction

Since the early 2010s, the creation, distribution and consumption of information in Thailand have shifted to online platforms due to the rapid popularisation of the internet. However, the policies of successive governments to gain control over the digital sphere have negatively impacted internet freedoms in the country. Coupled with persisting issues like disinformation, online harassment, and information operations, the internet has not reached its full potential to bring about democratic development in Thailand. Against this backdrop, this report examines the laws and measures that Thailand has adopted to regulate the online sphere, showing that a set of legal and non-legal measures have had a negative impact on internet freedom in the country. The report concludes with a set of policy recommendations to start improving internet freedoms in the country.

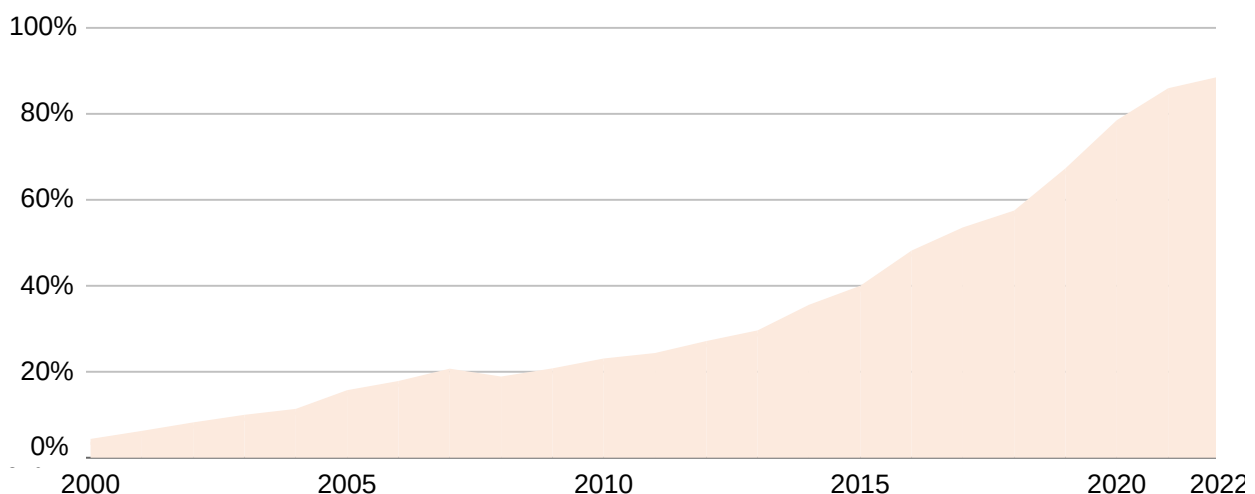
## 1a. Methodology

To elaborate this report, the research team conducted desk research between August and September 2023 to analyse three Asia Centre's publications about internet freedoms in Thailand through a policy perspective: *Thailand Computer Crime Act: Restricting Digital Rights, Silencing Online Critics* (2022a); *Internet Freedoms in Thailand* (2022b); and *State-sponsored Online Disinformation: Impact on Electoral Integrity in Thailand* (2023). News from both local and international outlets were also considered in examining the latest developments of the issues and policies presented in this report. The Asia Centre research team internally reviewed and obtained feedback from NDI Thailand to make necessary adjustments before its final submission.

## 1b. The Internet and Thailand's Political Development

The development of the internet sphere in Thailand started to become noticeable in the mid-2000s with a sharp increase in internet penetration. In 2011, 23.6% of the people in Thailand were internet users, while in early 2023, the internet penetration index had increased to 88% (World Bank, 2023). With the popularisation of the internet, the use of social networking sites (SNS) or social media also increased exponentially, particularly with the use of smartphones. At the start of 2023, there were 52.25 million social media users or 72.8% of the 71.75 million people living in the country. Aside from messaging applications like Line and Messenger, the most used SNS were Facebook, TikTok, and Instagram (Kemp, 2023).

Internet Penetration in Thailand (2000–2022)



The widespread use of the internet rapidly intersected virtually every aspect of the daily life of Thai people, including politics. Access to information from a range of sources became increasingly democratised and people could receive the news on the latest political developments almost instantly. In 2023, 64.9% and 58.1% of the people aged 16-64 who took part in a survey about internet use said that they used the internet to “find information” and “keep up-to-date with news and events”, respectively (*Ibid.*). Given the range of new possibilities that the internet offers to many people through their mobile devices and the potential impact that this might have on the politics of the country, successive governments have developed different strategies to cope with this situation with the regulation of the internet, thus adding a new layer into the development of the digital sphere in Thailand.

From 2014 to 2019, Thailand was ruled by the National Council of Peace and Order (NCPO), a military junta headed by General Prayuth Chan-o-cha. This period was marked by the efforts of the NCPO to consolidate its political power after the military takeover in 2014. These efforts included online platforms given the digital trends. The military amended the Computer Crime Act (2017) and doubled down the usage of existing laws such as Article 112 (*lèse-majesté*) and Article 116 (sedition) of the country’s Penal Code to regulate the information flow online, particularly concerning issues related to keeping accountability of government officials and policies. This was particularly noticeable on SNS, where most of these actions took place.

This period also saw the early usage of state-sponsored online disinformation campaigns to propagate pro-military narrative and discredit vocal critics and opponents – later known as “information operations (IO)” – by the Internal Security Operations Command (ISOC) (*Asia Centre, 2023*). Starting in 2014, the practice was first put into use in the Muslim-majority three southern border provinces, against local human rights defenders who advocated for the rights to self-determination and freedom of religion and belief, before it was institutionalised and implemented nationwide. It is noteworthy that the ISOC’s expanded role in policing the internet and propagating disinformation was enabled by the Internal Security Act – legislation passed by the Council for National Security, the military junta that staged a coup in 2006. The law further assigned the ISOC with vaguely worded tasks such as preserving the monarchy as the state institution and maintaining social cohesion. Practically, this means the ISOC could intervene in domestic politics in some capacities that were traditionally exercised by a civilian administration.

From 2019 to 2022, the leadership of the NCPO transformed into the Palang Pracharath Party (PPP), which, despite finishing second in the 2019 General Election, formed and led the coalition government. This period witnessed the sophistication of means to curb internet freedom, such as requests to tech companies to comply with content removal requests, strategic litigation against celebrities with lighter sentences, the practice of doxing, and the use of state-of-the-art Pegasus spyware to surveil political dissidents (*iLaw, 2022*). The uptake in political prosecution was attributed to the increasing internet penetration and, most importantly, the use of online platforms to keep public officials accountable – especially after the dissolution of the Future Forward Party (FFP) and during the COVID-19 pandemic when public gatherings were banned.

In the early 2020s, the pandemic increased the daily time that people spent surfing the internet to 11 hours, shifting from 10 hours just a year earlier (*Thansettakij, 2021*). Sources online also became the main source most Thai people use for news consumption (91%) (*Newman et al., 2021*). Kid for Kids (*2022*), a policy institute on youth, surveyed young people aged between 15 to 25 years old and found that online youth activism increased, with 67.5% of respondents to the survey reacting to political posts on social media. Additionally, 35.5% of the respondents create political content themselves in 2021. This corresponded with the birth of social media accounts of youth groups that coordinated the intermittent public protests from 2020 to 2021. These accounts – totalling 3,264,000 followers alone on Facebook – soon matured into a social infrastructure for political activism, informing and coordinating political mobilisation and solidarity actions in post-pandemic Thailand.



In May 2023 the Move Forward Party (MFP) won the General Election. In this context, the internet played a crucial role as the success of the party could be attributed to the Thai youth who, apart from being their main voters, are organic influencers and help canvass the votes for MFP through user-generated content on TikTok. This new social media platform can correspond well with local sensibilities thus multiplying engagement rates across various social strata ([Smith, 2023](#)).

Nonetheless, in September, a new coalition government emerged led by the Pheu Thai Party (PTP) – a coalition made possible by PTP joining hands with pro-military political parties. The new administration will be responsible for addressing issues related to internet freedoms in the country like disinformation, the impact of Artificial Intelligence (AI)-generated content, and information operations. It will also be tasked with addressing legacy measures used to regulate the internet in the last decade, which the next chapter addresses.

## **1c. Trust in Public Institutions**

In 2022, the King Prajadhipok's Institute, in partnership with the National Democratic Institute (NDI), conducted 32 focus group discussions across Thailand to support public and political will to strengthen the country's democratic governance and understand public attitudes toward key political institutions.

The most prominent public institutions that Thai citizens identified with Thailand's democracy were as follows: judiciary, parliament and political parties, and the media. There is also a heavy emphasis on educational and family institutions, connecting the relationship and providing bridges between Thai culture and the development of democracy. There is a sense that civic education is imperative for younger generations to have informed opinions on democratic values and practices.

When asked whether the House of Representatives and Senate work in the interest of citizens, most (about two in three) felt the House does not; the same is true for the Senate but with aggravated response (nine in ten). While the need for a check-and-balance function of the Senate is generally accepted, most see an election as the most appropriate way to select the senators, compared to appointments. The unpopularity of the current Senate, which was wholly appointed by the military, led to almost half indicating that the Senate should be disbanded altogether; to make them feel more democratically represented.

The dynamic emergence of political parties in Thailand has been a force in the democratisation and development of the country. As of now, except for older people, most citizens do not trust political parties; while about half trust them with some expressing faith or hope. Nevertheless, citizens commend political parties for providing social harmony uniting people with shared ideals, giving entry to interested and qualified individuals to participate in national politics and the development of efficient public policies.

Few trusted the media, with a focus on the privately-owned media. Many cited these media outlets profit from stirring things, without regard for the truth, and are not held accountable. After competing media outlets create confusion, citizens are left to conduct their research to find the truth. Again, these types of media stunts are in stark contrast to the Thai values of honesty and kindness. Some indicated the media had been intimidated by the government following the coup, which led to a cascading silence of expression.

## 2. Internet Freedoms Regulatory Measures

This chapter outlines two types of measures that have been systematically used to regulate the use of the internet in Thailand and, as a result, have impacted internet freedoms in the country. The first half of the chapter identifies the legal provisions that successive governments have used to increase their control over the online sphere. The second half of the chapter delves into the use of non-legal measures that have equally curbed internet freedoms. Additionally, the impact that these measures have had on certain individuals and organisations is also explained.

### 2a. Legal Measures



While freedom of expression, and by extension its exercise on online platforms, is guaranteed under the Constitution, a number of vaguely worded laws contain provisions that could be interpreted in an arbitrary manner and used to limit online freedom. This section reviews the Penal Code, the Computer Crime Act, and the Internal Security Act by examining problematic provisions and raising attention to applicable penalties for the infringement.

#### Penal Code

Certain provisions under Thailand's Penal Code (1956) criminalise the exercise of freedom of expression, including the online sphere. These provisions include Section 112 (lèse-majesté), 116 (sedition), 326 and 328 (defamation).

The former – Sec. 112 – reads “whoever defames, insults or threatens the King, the Queen, the Heir-apparent or the Regent, shall be punished with imprisonment of three to fifteen years”. This article has raised several concerns due to its vague wording, which could result in arbitrary enforcement. Here, the act of “insult” is not spelt out nor identified, thus leaving its interpretation in the hands of the local authorities. Another problem is the law does not set up clear thresholds to be met before the complaint can be brought before the court. In other words, it allows anyone to be a plaintiff to prosecute any individuals that they deem disrespectful towards the monarchy, regardless of fact or intention.

Regarding the latter, Section 116 (sedition), criminalises “whoever makes an appearance to the public by words, writings or any other means which is not an act within the purpose of the Constitution or for expressing an honest opinion or criticism to bring about a change in the laws of the country or the Government by the use of force or violence; raise unrest and disaffection amongst the people in a manner likely to cause disturbance in the country; or cause the people to transgress the laws of the country” with imprisonment no more than 7 years. Again, the provision uses vaguely worded provision, which leaves room for unpredictable interpretation by authorities. For example, no specific explanation is made to clarify what action may constitute “disaffection ... in a manner likely to cause disturbance”.

Criminal defamation is stipulated under the Penal Code in addition to the Civil Code. Most of the provisions that have been used to harass political dissidents or silence critics include the following:

Section 326 criminalises “whoever imputes anything to the other person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to be hated or scorned” with imprisonment no more than one year or fine no more than THB 20,000 (USD 595), or both.

Article 328 builds on Article 326 to criminalise the act of defamation by publication. This covers defamation “by means of publication of a document, drawing, painting, cinematography film, picture or letters made visible by any means, gramophone record or another recording instruments, recording picture or letters, or by broadcasting or spreading picture, or by propagation by any other means”. Penalty includes imprisonment not exceeding two years and fine not exceeding THB 200,000 (USD 5,945).

### Computer Crime Act

In 2007, with the increasing use of the Internet for commercial activities, the Computer Crime Act (CCA) (2017) was originally introduced to tackle cybercrimes such as phishing and online data farming (Achavanuntakul, 2015). Still, with some vaguely worded provisions, the law becomes highly subjective and open to multiple interpretations that can criminalise freedom of expression (iLaw, 2013). In December 2016, an amendment to the CCA was enacted to address the use of the CCA as defamation lawsuits between private citizens and between public officials and individuals and empower the authorities to control online harmful content (iLaw, 2016).

Sections 14, 15, 18, and 20 of the CCA have become contentious for their restriction of internet freedom by allowing for the prosecution of internet users and internet service providers (ISPs). Article 14 of the CCA stipulates up to five years of imprisonment or a fine of no more than THB 100,000 (USD 2,972) or both, for “entering ... distorted or false computer data ... deemed to cause damage to the general public, national security, public safety, economic safety or to cause panic to the general public”. This includes the crime of “disseminating or forwarding such computer data”. However, this provision does not provide a clear definition of what is distorted or false information and does not specify what kind of information can cause damage.

Under Article 15, “a service provider, who cooperates, consents or supports the perpetration of the offences” is liable for the same penalty as the offender under Section 14 of the Act. In this case, the MDES can issue a notification specifying the process of warning, blocking the dissemination and removal of such computer data (known as the “notice and takedown mechanism”).

Article 18 delineates the powers vested in officials under the Act. These powers encompass a range of actions, including the ability to request statements from individuals involved in the commission of an offence (Subsection 1) and the authority to request computer traffic data from service providers (Subsection 2). Furthermore, officials are empowered to order service providers to furnish information regarding their clients (Subsection 3) and to duplicate computer data and computer traffic data from computer systems suspected of being utilised in an offence (Subsection 4). They can also issue directives for the provision of computer data or devices by the computer data processor, controller, or storage device owners (Subsection 5). In addition, officials have the prerogative to inspect or access computer systems, computer data, computer traffic data, or storage devices as evidence related to the offence (sub-section 6) and decode computer data of individuals (Subsection 7). Lastly, they possess the authority to seize or attach any computer system for investigation and evidence gathering (Subsection 8).

Article 20 provides that the official, with approval from the Minister (of the Ministry of Digital Economy and Society), may file a petition to the court to halt dissemination or to remove the data in question. Such power applies to any computer data that compromises the security of the country, relates to other criminal laws and breaks the public order or good morals. In an action that is deemed to be a breach of the public order or good morals of the people, the Minister has the power to file a petition to the court to suppress the dissemination or to remove the computer data.

The CCA is intrinsically problematic. Its provisions contain vague language that is subject to varied interpretations and the discretion of the authorities. Furthermore, it is implemented selectively to block or remove undesirable content and prosecute individuals who express opinions against the establishment or monarchy. Often, the Act is used by the authorities to harass internet users and create an atmosphere of fear, leading to self-censorship.

### **Internal Security Act**

Examining the Internal Security Act (ISA) (2008) is essential because the law provides a legal basis for the institutionalisation of state surveillance and information operations under the name of national security. It is the Internal Security Operations Command (ISOC) that takes action on these policies and practices that stifle key human rights in the online sphere.

Article 5 of the ISA designates ISOC to report directly to the Office of the Prime Minister. It designates the prime minister as the Director of ISOC and the Chief of Staff of the Army as his or her deputy director.

Article 7 outlines the tasks and mandates of the ISOC as to “monitor and analyse incidents that may jeopardise internal security of the Kingdom, ... lead on internal security affairs and present policies and practices to the prime minister for approval ... encourage public awareness in safeguarding nation, religion and King and preserving social harmony, or to act upon any assignments requested by the prime minister, the cabinet and the National Defence Council”.

Articles 11 and 13 allow for the creation of ISOC’s directives at regional and provincial levels. Both Articles contain provisions that allow for the inclusion of civilian staff in the locality to operate under the ISOC local directives.

Noticeably, the main problem with ISA is that it creates a “state-within-state” or “deep state” condition bypassing the national civilian administration. The ISOC is akin to an alternative government with its management system at regional and local levels under the leadership of regional military commanders with little to no accountability.

## **2a. Non-legal Measures**

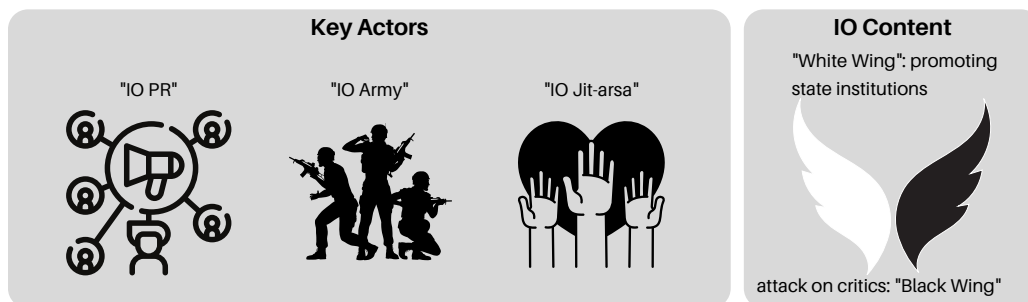
With the legal framework provided by ISA, ISOC directives possess the flexibility to adopt measures to address potential threats to national security and the monarchy. ISOC's proactive measures are typically implemented through two distinct approaches: information operations (IO) and state surveillance, both of which leverage the existing infrastructure at their disposal.

### Information Operations

In Thailand, information operations are carried out by a range of actors, including state agencies, private or public relations companies, and pro-establishment volunteers. These actors create and spread disinformation to manipulate public opinion and target dissidents and pro-democracy supporters. IOs aim to discredit opponents, spread hate speech, and distort facts, creating social disharmony and reinforcing the establishment's power. From a parliamentary session in 2020, Wiroj Lakkhanaadisorn, a member of parliament of MFP, alleged that the ISOC allegedly operated between 19 to 40 cyber units comprising over 1,000 rank-and-file army personnel ([Prachatai, 2020](#)). A target is set at an hour per day for five-person units to influence or manipulate online content on social media platforms ([Sombatpoonsiri, 2022](#)). In 2020, it was reported that some public relations firms which have close ties to senior military leadership were contracted to improve the reach and engagements of IO content ([Matichon, 2020](#)).

IO campaigns can be categorized as "black" or "white". "Black" discredit government dissents and opposition party members. "White" propagate pro-government content ([Inkutanonda, 2021](#)). In practice, an IO operator often manages several social media accounts using fake accounts to monitor prominent social activists, members of the opposition and human rights defenders, and observe online discussions in social media groups to get a sense of ongoing contentious issues. Once targets are identified, operators reshare targeted content and add pro-military and pro-monarchy views to the original content in an attempt to debase its intellectual vigour.

### Ecosystem of State-sponsored IO in Thailand



Before nationwide application, information operations were first tried and tested in the Muslim-majority three southern border provinces by Region 4 Forward Command of ISOC. Using Facebook pages and website (Pulony), the military disseminated fake news and hate speech against human rights defenders, politicians, and local CSOs peacefully advocating for the right to self-determination, framing them as instigators who want to secede from Thailand and declare independence ([Isranews, 2014](#)). Apart from day-to-day online surveillance and reactionary response, the IO units are latent networks the government can activate to engage dissenting views in anticipation of major politically sensitive events such as the dissolution of the Future Forward Party, or the 2020 student-led protests. It is estimated that during the nationwide protests in 2020, the number of fake Twitter accounts engaging in inauthentic behaviour and information operations could reach 17,562 ([Beattie, Thomas & Zhang, 2020](#)).

### Targeted Surveillance

From 2020 to 2021, it was estimated that at least 30 Thai pro-democracy activists and scholars were subject to attacks from a state-sponsored digital intrusion. Known for its advanced, sophisticated technology, the zero-click Pegasus spyware can access and harness personal data from one's phone for a third party without the user clicking dubious, malicious links. It can copy messages users send or receive, and record their outgoing or incoming calls, with the phone's camera and microphone secretly switched on beyond users' control ([Cutler & Pegg, 2021](#)). Hence, it can potentially pinpoint the location of its target,



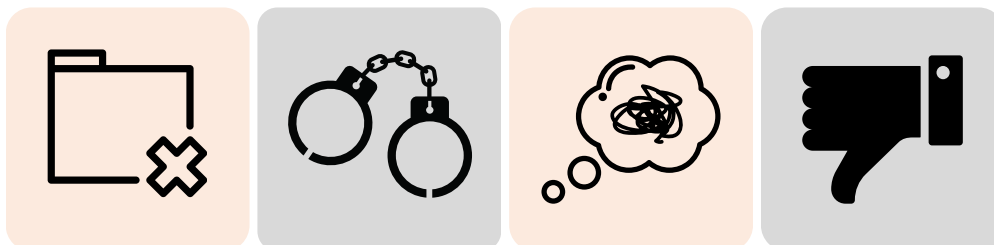
who they have interacted with, and the exact conversation they share. Pegasus was developed by an Israeli cybersecurity firm NSO Group, which enjoys close relationships with Israel's Military Intelligence Directorate.

### The Use of Spyware Pegasus



According to iLaw's report, the use of Pegasus against activists, government critics and members of civil society could be attributed to three main reasons: to monitor the online activities of targets; to monitor the protests; and to seek information about the funding sources for the protests ([iLaw, 2022](#)). It is worth noting that the Pegasus attacks coincided with the student-led mass protests in 2020, where most of the individuals under attack participated and demanded a monarchy reform. The government denied any involvement but accepted that similar technology is used in national security matters and anti-narcotic operations ([Reuters, 2022](#)). In 2023, activists sued government agencies for the alleged use of Pegasus spyware to gain access to their phones and personal data ([Saksornchai, 2023](#)).

## 2c. Impact



Vaguely worded provisions under the Penal Code, the CCA, and the ISA do not meet international standards and allow legal abuse to occur. From direct persecution of online critics, and denying access to online critical content, to harassment, these laws have had a significant impact on Thai citizens' internet freedoms.

### Persecution of Users

Internet users who use social media platforms to keep government officials and policies accountable, as well as mobilise the public with political aims, have been persecuted under the laws examined in the previous chapter. From July 2020 to July 2023, to curb public dissent and call for institutional reform, at least 1,918 people have been prosecuted in 1,230 cases due to their political participation and expression, including 286 youngsters aged below 18 years old ([Thai Lawyers for Human Rights, 2023](#)). As the CCA allows for compounded punishments for offences stipulated under the Penal Code, some were charged more than once. Notable examples include political activist Parit Chiwarak who has collected more than 23 criminal charges by the end of 2021.

During the COVID-19 pandemic, the government tried a new tactic to file defamation lawsuits against celebrities who called out the mismanagement of the public health crisis. This was to set an example and

keep the combustible public in line. Sontiya Sawasdee, the prime minister's lawyer, had listed more than 20 celebrities he intended to file complaints against (BBC, 2021). The most infamous case was the Thai rapper and singer Danupha Khanatheerakul, better known by her stage name "Milli", who was fined for defamation (Ibid).

These developments have directly led to a chilling effect on freedom of expression in Thailand and the acute culture of self-censorship practised by the media and individuals, especially online. As one journalist notes, "there are unwritten, unspoken rules on news reporting in Thailand: avoiding reporting on the government's violent crackdown on fundamental rights and protesters, and the Thai monarchy" (Thanalertsomboon, 2021). Impartiality is exclusively interpreted as a reportage of objective 'facts' devoid of opinion or political analysis.

### Denying Access to Information

The CCA enables the government to pressure technology companies to block and remove online critical content it deems controversial and may affect national security. Most of the targeted content and sites were related to criticisms against the government and monarchy as well as political mobilisation. In 2020, the Ministry of Digital Economy and Society revealed that the court issued an order to suspend 13,505 URLs that allegedly commit the lèse-majesté offences. These numbers can be categorised per the following: Facebook (7,990), YouTube (3,058), Twitter (1,070), and other websites (1,387) (Post Today, 2020).

Facing the threat of being forced out of the country, technology firms have little choice but to comply. To illustrate, between July and September 2021, the government made 162 requests to remove 436 items across various Google services, 70% of which were removed. Note that 96% of the complaints were criticism directed at the government (Google, 2021). Facebook fared no better in the same period as it decided to restrict access to 77 posts allegedly violating Section 112 under the Penal Code (Meta, 2021). Twitter, however, stood firm and committed to protecting the right to access information as it complied with only 12% of 50 legal requests to remove content from 130 accounts in the same period (X, 2021).

In 2022, from January to June, the MDES sought court authorisation and cooperation from social media platforms to block over 2,630 websites, 47% of which were removed for allegedly insulting the monarchy. According to Facebook's Transparency Center, the platform restricted access to 2,240 items in Thailand between January and June 2022. Data from the Google Transparency Report from the same reporting period reveals that there have been 419 requests for content removal from YouTube, citing government criticism. It is noteworthy that websites providing means to circumvent censorship or restrictions on content have been blocked by local telecommunications companies (telco). For example, VPN Hotspot Shield used to be blocked by TRUE, and Ultrasurf was blocked by DTAC, AIS and 3BB as of 2021 (Freedom House, 2022).

### Mental Health

In 2023, the Monitoring Centre on Organised Violence Events, surveyed digital harassment against Thai human rights defenders (HRDs). It revealed that HRDs expressed that online harassment, especially IOs, has an impact on their mental well-being (67%). Often it started from online naming and shaming incidents before transcending into day-to-day, physical harassment. A pro-democracy activist Joe (not his real name) stated that after a doxxing case when a person published his phone number and his home address on Facebook, he had received threatening calls for months, precipitating him to develop mental health issues (Amarinthewa, 2023).

Amad (not his real name), a human rights activist in the three southern border provinces, has been subjected to IO accusing him of being a Muslim separatist. This led to physical surveillance being placed

upon him. Eventually, he was called in for questioning and tortured while under military custody. This led to physical surveillance being placed upon him. Eventually, he was called in for questioning and tortured while under military custody. The whole ordeal has left him with post-traumatic stress disorder (PTSD) (Ibid.). A feminist Noon (not her real name) shared her experience when facing the IO disrupting the online event. This included death and rape threats and derogatory remarks that flooded the online discussion leading to the cancellation of the event. She sought help after she felt overwhelmed and had an urge to commit suicide in protest (Ibid.).

While the impact of the use of legal measures to prosecute government critics, activists and online users based on their political expression is well-recorded through several court cases, the psychological toll on their mental well-being is less clear and understudied. Social stigma on mental health patients also complicates this issue, which can potentially subject the HRDs to double discrimination.

### **Declining Trust in Public Institutions**

The uptake in court prosecutions and charges against human rights defenders, vocal critics and internet users based on their online political expression, when combined with a chilling effect on the domestic mainstream media who practise self-censorship, has resulted in declining trust in public institutions associated with rule of law and democratic governance in Thailand.

First, trust in the judiciary is at its lowest ebb, because the administration of justice, especially those involving freedom of expression and the Constitution, is very politicised and does not proceed according to international standards or what has been taught at universities ([The 101world, 2021](#)). Offences under Section 112 (*lèse-majesté*) and the Computer Crime Act were used in tandem to compound punishment upon the accused. In addition, the internationally accepted principle of “innocent until proven guilty” was often ignored, when *lèse-majesté* offence is concerned. This often led to the right to bail being unreasonably denied, although such a right is guaranteed under the Constitution.

In 2022, a focus group discussion conducted by the King Prajadhipok's Institute (KPI) revealed that only a few trusts the media and the legislature (political party system and MPs) in Thailand. The finding is even more acute among younger generations when breaking down. As coverage on sensitive, political issues such as online public criticism, protests and solidarity actions of activists are censored, journalists shift to sensational reporting or stories that would create virality of content without regard to truthfulness or public morality. This inadvertently encourages misinformation and degradation of journalist ethics – resulting in declining trust from the public.

Plagued by intraparty factionalism in the lower house and military-appointed Senate, hope for social change or better protection of fundamental human rights through the legislature is equally frustrated. In 2021, proposed by the Move Forward Party, draft amendments to Section 112, the CCA, and the draft law on miscarriage of justice were either rejected outright or stalled in the National Assembly by political parties or senators that were supported by the military. These laws are pertinent to the promotion and protection of internet freedom in Thailand. Per the focus group discussion, except in Northeastern and Eastern parts of Thailand, very few people have trust in the legislature.

## 3. Policy Recommendations

This report has outlined how certain governmental actions to remain in control of the online sphere have contributed to the erosion of internet freedom in the country while contributing to a trust crisis from the public to public institutions. This chapter presents a set of recommendations aimed at a range of state and non-state actors to identify solutions that can start fixing this problem.

### Development aid agencies and diplomatic missions – should:

- Use diplomatic channels to convey concerns from CSOs and online users to the Thai authorities on the detrimental effects of information operations.
- Engage through UN mechanisms such as UPR, SRs, and OHCHR working groups to request Thailand to cease its Information Operations that impact civil and political rights.
- Use human rights mechanisms such as the UPR, SRs and OHCHR working groups to engage with the Singapore government to persuade it to address human rights violations in the online sphere, as recommended by member states in their UPR submissions.
- Engage with technology companies to ensure their moderation policies are transparent and effective to either remove or block harmful content.

### The government should:

- Constructively engage with the international community, through the UN mechanisms and through dialogue with other relevant stakeholders, to receive feedback and implement suggestions on the country's human rights obligations.
- Refrain from using the CCA to prosecute legitimate expression in the online space, or to compound punishment in tandem with other offences in the Penal Code such as lèse-majesté (Section 112), or sedition (Section 116).
- Enforce Section 161/1 and 165/2 of the Criminal Procedure Code to prevent harassment or lawsuits against individuals due to their legitimate expression.
- Review and ensure that the functions of the Anti-Fake News Centre are aligned with international standards such as the International Fact-Checking Network (IFCN) Codes and Principles.
- Answer factually in Parliament questions or motions related to Information Operation.
- Exercise professionalism and support opposition parties' efforts in amending and repealing problematic laws that infringe on internet freedom.
- Raise awareness that public figures, including those exercising the highest political authority and highest moral authority, are legitimately subject to criticism.

### The Parliament should:

- Review and amend Section 14(2) of CCA, deleting vague language and providing clear definitions or specifications to avoid arbitrary and overbroad interpretations.
- Repeal Section 14(3) of the CCA, which overlaps with provisions in the Penal Code.
- Amend Section 15 from imposing strict liability offence to include the intentionality requirement for committing an offence.
- Amend Section 18 of the CCA to specify that information requests of the authorities must be authorised by the court.
- Section 26 of the CCA should establish a mechanism for protecting privacy and guarantee that data accessed by the authorities are under legal protection.

- Increase transparency and judicial examination in the appointment of the officials who execute the provisions of the CCA.
- Amend Articles 34, 35 and 36 of the Constitution, eliminating vague and ambiguous language so that these Sections can be used to protect internet freedom appropriately. Amend exceptions to Articles 34, 35 and 36 of the Constitution to align them with international human rights standards considering principles of necessity, proportionality and non-discrimination.
- Repeal or significantly amend Sections 112 (lèse-majesté) and 116 (sedition) of the Penal Code that contains vague and ambiguous language open to arbitrary and extensive interpretation and which do not align with international human rights standards.
- Decriminalise defamation under Articles 326, 327 and 328 of the Penal Code and situate it solely within the Civil Code.
- Repeal the Internal Security Act to cease information operations perpetrated by the ISOC.

### The NHRCT should:

- Proactively oversee the allegations of harassment, prosecution and other forms of human rights violation against internet users.
- Provide expert opinion to government agencies to ensure that their operations are aligned with international human rights standards.
- Engage with parliamentarians through parliamentary mechanisms, such as the annual report session or parliamentary committee, to take feedback and suggestions to improve the execution of its mandate.

### The ECT should:

- Increase engagement with political parties and CSOs to take feedback and update electoral regulations, ensuring the practicality of requirements and their alignment with international standards.
- Explore partnerships with technology companies on fact-checking mechanisms to combat online disinformation during election seasons.

### CSOs should:

- Monitor, document and call out incidents of harassment and prosecutions through domestic and international mechanisms.
- Provide risk assessment assistance to human rights defenders and activists.
- Engage national and UN human rights mechanisms.
- Provide digital literacy to the public to help them better protect themselves from disinformation.
- Work closely with tech companies to assist them in detecting cases of Information Operations and also in combating them.
- Initiate alternative fact-checking mechanisms for the public.

### Technology Companies should:

- Institutionalise human rights standards when developing or updating software and platforms, especially those that are related to online privacy.
- Publicise their detailed transparency reports enumerating all removing and blocking requests by the government.
- Engage with CSO to jointly promote the protection of online users, especially from online surveillance and spyware.



## 4. Conclusion

Today, the internet has become an essential foundation for numerous daily tasks in our ever-more digitised societies. From a rights perspective, it has created many new opportunities for advocating human rights. However, it has also introduced new challenges that cannot be ignored to ensure the preservation of internet freedoms in the country. This is one of the key challenges that the newly elected government following the May 2023 elections will have to address.

In Thailand, internet freedoms are in jeopardy. Since the early 2000s, successive governments, cognisant of the digital being becoming a game-changer for the social and political development of the country, have increased their efforts to tighten their control over online content. As a result, internet freedoms have decreased and, overall, people's declining trust towards public institutions, particularly the judiciary, has increased.

The legal ecosystem has been used to regulate people's digital activity with existing laws like the Penal Code. Additionally, new legal provisions like the Computer Crime Act have been passed in response to the recent technological developments to further regulate the digital sphere. However, the use of the law to accomplish this purpose has presented several challenges since some people and organisations trying to keep government officials and policies accountable have been criminalised because of their actions.

Non-legal measures to regulate the online sphere have also raised concerns regarding the state of internet freedoms. Information operations and targeted surveillance have resulted in certain political actors being discredited and the online activity and safety of key actors being compromised, respectively.

These actions have had a significant impact on internet freedoms across multiple fronts. Many individuals engaged in advocacy and activism have reported persecution, and some have encountered increasing difficulties in accessing vital information. This has been facilitated by the government's use of critical laws like the Computer Crime Act to block or restrict the flow of information. Additionally, these actions have taken a toll on the mental health of many individuals, making it more challenging for them to continue their activities. From a broader perspective, these developments have also eroded trust in government institutions. Trust has not only diminished but has also widened the gap between state and non-state actors, which undermines both internet freedoms and democracy within the country.

The newly elected Thai cabinet will need to address them to ensure that internet freedoms in the country are respected and social cohesion is improved. The 2023 general election has seen the pro-democracy Pheu Thai Party (PTP) forming a coalition with the military and centre-right parties, making it challenging to amend problematic laws or change policies. However, substantial change is possible through a multi-stakeholder approach that involves state and non-state actors - the international community, the parliament, the ECT, NHRCT, CSOs, and tech companies - engaging in dialogues with one another to reach consensual solutions. It is only through the engagement of such a variety of stakeholders that Thailand will move in the right direction to create an online environment where everyone's rights are fully respected.

---

# BIBLIOGRAPHY

Asia Centre (2022a), *Thailand Computer Crime Act: Restricting Digital Rights, Silencing Online Critics*, Bangkok: Asia Centre, [https://asiacentre.org/wp-content/uploads/Thailand-Computer-Crime-Act\\_Restricting-Digital-Rights-Silencing-Online-Critics.pdf](https://asiacentre.org/wp-content/uploads/Thailand-Computer-Crime-Act_Restricting-Digital-Rights-Silencing-Online-Critics.pdf).

Asia Centre (2022b), *Internet Freedoms in Thailand, Silencing Online Critics*, Bangkok: Asia Centre, <https://asiacentre.org/wp-content/uploads/Internet-Freedoms-in-Thailand-2022.pdf>.

Asia Centre (2023), *State-sponsored Online Disinformation: Impact on Electoral Integrity in Thailand*, Bangkok: Asia Centre, <https://asiacentre.org/wp-content/uploads/State-Sponsored-Online-Disinformation-Impact-on-Electoral-Integrity-in-Thailand.pdf>.

Achavanantakul, Sarinee (2015) “พัฒนาการ” ของการตีความ พ.ร.บ. คอมพิวเตอร์ [“Development” of the interpretation of the Computer Crime Act], ThaiPublica, at: <https://thaipublica.org/2015/09/computer-law-progress>.

Amarinthewa, Wongphan (2023) “อาการนี้จะติดตัวเราไปจนตาย” ไอโอ-การคุกคามออนไลน์ ผลทำลายล้างสุขภาพใจของนักเคลื่อนไหวการเมือง [“This symptom will accompany us until death” IO-Online Threats damage mental health of political activists], The 101 World, at: <https://www.the101.world/digital-harassment-mental-devastation>.

BBC (2021) ‘ดาราคall out: นายนาทฯ แจ้งความ “มิลลิ” ข้องหาหมิ่นประมาท หลังวิจารณ์รัฐบาลประยุทธ์ [Celebrities calling out: Prime Minister’s lawyer files complaint against Milli for defamation after criticising the Prayut government]’, BBC News Thai, at: <https://www.bbc.com/thai/thailand-57925336>.

Freedom House (2022) ‘Freedom in the World 2022: Thailand’, Freedom House, at: <https://freedomhouse.org/country/thailand/freedom-world/2022>.

Google (2023) ‘Government requests to remove content’, Google Transparency Report, at: <https://transparencyreport.google.com/government-removals/overview>.

iLaw (2013) ‘The Research on the Impact of the CCA 2007’, iLaw, at: <https://ilaw.or.th/node/1798>.

iLaw (2016) ‘ร่างแก้ไขพ.ร.บ.คอมพิวเตอร์ฯ “ตั้งคณะกรรมการปิดเว็บแม้ไม่ผิดกฎหมาย” [Draft amendment to the Computer Crimes Act, “Sets up a committee to shut down websites even if they are not illegal”]’, iLaw, at: <https://ilaw.or.th/node/4092>.

iLaw (2022) ‘Parasite that Smiles: Pegasus Spyware Targeting Dissidents in Thailand’, iLaw Freedom, at: <https://freedom.ilaw.or.th/en/report-parasite-that-smiles>.

Ingkuthanon, Trinuch (2021) “มหากาพย์ไอโอ” เมื่อภาษีประชาชน ถูกใช้ด้วยคำประชาชน? [“The IO epic” When taxes on citizens, are used to devalue the people?], Thairath Plus, at: <https://plus.thairath.co.th/topic/politics&society/100402>.

Isra News (2014) ‘ไอโอ “ล้ำเส้น” ที่ชายแดนใต้ [IO “crosses the line” at the southern border]’, Isra News, at: <https://www.isranews.org/content-page/item/34484-io.html>.

---

Kemp, Simon (2023) 'Digital 2023: Thailand', Datareportal, at: <https://datareportal.com/reports/digital-2023-thailand>.

Kid for Kids (2022) 'เด็กและเยาวชนมีส่วนร่วมทางการเมืองแต่ภาครัฐสกัดกั้นด้วยความรุนแรงมากขึ้น [Children and youth participate in politics, but the government sector blocks participation through violence]', Kid for Kids, at: <https://kidforkids.org/child-and-family-situation-report-2022/political-participation>.

Matichon (2020) "'ก้าวหน้า" จัดหนัก แจก 54,000 บัญชีทหารทำ IO เปิดชื่อเอกชนร่วมทหาร ทำครบวงจร [“Progressive Movement” reveals 54,000 military accounts doing IO, revealing the names of private companies joining the military – a complete system]', Matichon Online, at: [https://www.matichon.co.th/politics/news\\_2467713](https://www.matichon.co.th/politics/news_2467713).

Meta (2023) 'Thailand', Meta Transparency Center, at: <https://transparency.fb.com/reports/content-restrictions/country/TH/?source=https%3A%2F%2Ftransparency.facebook.com%2Fcontent-restrictions%2Fcountry%2FTH>.

Newman, Nic, Richard Fletcher, Anne Schulz, Simge Andi, Craig T. Robertson, and Rasmus Kleis Nielsen (2021) *Reuters Institute Digital News Report 2021*, Reuters Institute for the Study of Journalism, at: [https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital\\_News\\_Report\\_2021\\_FINAL.pdf](https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf).

Pegg, David and Sam Cutler (2021) 'What is Pegasus spyware and how does it hack phones?', The Guardian, at: <https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones>.

PostToday (2020) 'ดีเอสไอ บล็อกแล้ว คดีหมิ่นฯ กว่า 13,505 ยูอาร์แอล [DES has blocked more than 13,505 URLs in defamation cases]', PostToday, at: <https://www.posttoday.com/economy/news/636943>.

Prachatai (2020) 'เปิดสไลด์ ส.ส.5โรจน์ อีกครั้ง เพจไหนเป็นเป้า บัญชีไหนเป็นหมายของ IO ทหาร [Opening MP's Wiroj's slide. Which pages are the targetted? Which accounts are targets for military IO?]', Prachatai, at: <https://prachatai.com/journal/2020/03/86617>.

Thai Lawyers for Human Rights (2023) 'July 2023: A total of 1,918 people have been politically prosecuted in 1,230 cases', Thai Lawyers for Human Rights, at: <https://tlhr2014.com/en/archives/59312>.

Thanalertsomboon, Pawan (2021) 'เมื่อสื่อติดกับดักความเป็นกลางและความกลัว - เปิดปมสื่อไทย ทำไมจึงปิดปากตัวเอง? [When the media is trapped in neutrality and fear - revealing the secrets of Thai media; Why do they keep their mouth shut?]', The 101 World, at: <https://www.the101.world/media-self-censorship>.

Thansettakij (2021) 'คนไทยเข้ายุคดิจิทัล โควิดดันยอดใช้เน็ตพุ่ง [Thai people enter the digital age; Covid increases internet usage]', Thansettakij, at: <https://www.thansettakij.com/technology/475214>.

The 101 World (2021) 'ฟื้นวิกฤตศรัทธา ถึงเวลาปฏิรูปกระบวนการยุติธรรม [Reviving the crisis of faith. It's time to reform the justice system]', The 101 World, at: <https://www.the101.world/thai-justice-system-reform>.

Thomas, Elise, Tracy Beattie and Albert Zhang (2020) '#WhatsHappeningInThailand: the power dynamics of Thailand's digital activism', *Quick take*, International Cyber Policy Centre, Australian Strategic Policy Institute.

Reuters (2022) 'Govt admits using phone spyware, cites "national security"', Bangkok Post, at: <https://www.bangkokpost.com/thailand/general/2350068/govt-admits-using-phone-spyware-cites-national-security>.

---

Saksornchai, Jintamas (2023) 'Thai activists sue government agencies for allegedly using Pegasus spyware against them', AP News, at: <https://apnews.com/article/thailand-surveillance-nso-spyware-1081ac34cf80e15c048af8c2d1db0e33>.

Smith, Serena (2023) 'The Move Forward party is bringing hope to Thailand's youth', Dazed, at: <https://www.dazeddigital.com/life-culture/article/59894/1/the-move-forward-party-thailand-youth-election-pita-limjaroenrat>.

Sombatpoonsiri, Janjira (2022) "'We are Independent Trolls': The Efficacy of Royalist Digital Activism in Thailand", *Perspective* 2022(1), ISEAS Yusof Ishak Institute, at: [https://www.iseas.edu.sg/wp-content/uploads/2021/12/ISEAS\\_Perspective\\_2022\\_1.pdf](https://www.iseas.edu.sg/wp-content/uploads/2021/12/ISEAS_Perspective_2022_1.pdf).

World Bank (2023) 'Individuals using the Internet (% of population)', World Bank, at: <https://data.worldbank.org/indicator/IT.NET.USER.ZS>.

X (2023) 'Thailand', X Transparency, at: <https://transparency.twitter.com/en/reports/countries/th.html>.

"Computer-related Crime Act" (2017), Thai Netizen Network, at: <https://thainetizen.org/docs/cybercrime-act-2017>.

"Internal Security Act" (2008), Office of the Councillors of the State, at: [http://web.krisdika.go.th/data/document/ext809/809941\\_0001.pdf](http://web.krisdika.go.th/data/document/ext809/809941_0001.pdf).

"Penal Code" (1956), Thailand Law Online, at: <https://www.thailandlawonline.com/table-of-contents/criminal-law-translation-thailand-penal-code>.

# RESEARCH SERVICES

*Asia Centre provides evidence-based research to bring impactful change to policies and improve human rights in Southeast Asia.*

## Key Research Areas Include:

- ▷ Freedom of Expression: Disinformation / Internet Freedoms
- ▷ Media: Press Freedoms / Media Information Literacy / Media Ethics
- ▷ Freedom of Religion and/or Belief
- ▷ Democracy & Elections
- ▷ Geopolitics of the Asia-Pacific Region
- ▷ Business and Human Rights
- ▷ International Development/Aid
- ▷ Enforced Migration
- ▷ Social Enterprise / Social Innovation

**Baseline Studies**

**Needs Assessments**

**Strategic Plans**

**Policy Reports and Briefs**

**Project Evaluations**



### Asia Centre Research Hub

65/168, Chamnan Phenjati Business Center Building, 20th Fl., Rama 9 Rd.,  
Huai Kwang, Huai Kwang, Bangkok 10310, Thailand



[asiacentre.org](http://asiacentre.org)



[contact@asiacentre.org](mailto:contact@asiacentre.org)







 Asia Centre

 Asia Centre

 Asia Centre

 @asiacentre\_org

 asiacentre\_org

 asiacentre

website: [asiacentre.org](https://asiacentre.org)

email: [contact@asiacentre.org](mailto:contact@asiacentre.org)

Asia Centre is a civil society research institute that seeks to create human rights impact in the region. Asia Centre's work focuses on issues related to civil society, democracy, elections, freedom of expression, freedom of religion or belief and human rights. The Centre believes that knowledge toolkits built from evidence-based research on critical human rights issues are important for designing activities for stakeholder capacity strengthening and making informed policy interventions. With this aim, Asia Centre was established in Bangkok, Thailand in 2015 and a second branch was registered in 2018 in Johor Bahru, Malaysia. On 21 May 2021, the Centre was recommended by the Committee on Non-Governmental Organizations of the UN ECOSOC for a Special Consultative Status.

To date, the Centre has been undertaking evidence-based research on key human rights issues to assemble knowledge tools such as books, reports, baseline studies, policy briefs, commentaries, infographics, videos and training programmes. These knowledge tools are often developed at the request of civil society, INGOs and parliamentarians for evidence-based research on critical rights challenges. These knowledge tools are then used to design capacity building programmes for stakeholders so that they can affect positive policy changes.